INFORMATION SECURITY

The security of a company’s sensitive information and data is vital to the continued functioning of the organization. It is the responsibility of everyone within the company to maintain a high level of awareness regarding information security.

Follow secure computing guidelines like maintaining password security, keeping anti-malware protection current and active, following good email practices, and adhering to all company security policies. Report any threats to the company’s sensitive and/or confidential information immediately. It only takes one security breach to threaten the reputation and future of a trusted organization.

SECURE COMPUTING DEADLINES

☐ Don’t open attachments or click on links within emails unless you know the sender and are expecting the attachment or link.
☐ Use passwords that are cryptic and combine multiple character types that can’t be easily guessed. Use different passwords for each system and application you log into.
☐ Check with your IT security team before downloading any new program or application. Don’t download programs from websites that you don’t know and trust.
☐ Don’t surrender personal or sensitive information to anyone or any website without verifying the authenticity of the requester. Think before providing any information that could be abused if it fell into the wrong hands.
☐ Always maintain current antivirus and anti-malware software. Make sure to update it regularly.
☐ Always keep operating systems, application updates, and security patches current.

THREATS TO A COMPANY’S INFORMATION SECURITY

☐ Email attachments can contain programs that may compromise the security of a computer. This can allow a cyber-criminal to access secure data files without detection.
☐ Links sent via email or social media may lead to harmful websites that can infect a computer with malware or viruses.
☐ Phone calls or messages can trick employees into revealing secure information. Never provide confidential or personal data without verifying the identity of the requester.
☐ Lost or stolen laptops, tablets, or electronic storage devices can provide access to a company’s secure network. Always protect devices and report them immediately if lost.

For further information on maintaining a culture of preparedness, consult your Preparis portal. Contact your Customer Success representative at csteam@preparis.com for more information on this or any other threat.